PATENT
Attorney Docket No. JP920020102US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Masayuki NUMAO et al.	Examiner: MORSE, Gregory A.
Serial No: 10/600,547	Art Unit: 2134
Filed: June 20, 2003	
For: INFORMATION DISTRIBUTION AND PROCESSING	

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF DATED APRIL 29, 2009

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notification of Non-Compliant Appeal Brief dated April 29 2009, the Appellants submit herewith a replacement Summary of the Claimed Subject Matter section of the Appeal Brief filed March 26, 2009. The replacement Summary of the Claimed Subject Matter section cites passages by page and line numbers rather than paragraph numbers.

No fee is believed due with this Notice, however, should a fee be required please charge Deposit Account 50-0510. Should any extensions of time be required, please consider this a petition thereof and charge Deposit Account 50-0510 the required fee.

Respectfully submitted,

Dated: April 9, 2009

/ido tuchman/

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (718) 374-6092

Summary of the Claimed Subject Matter

Independent claim 1 recites an information distribution system. Application, pp. 6, ll. 14-16, Fig. 1. The information distribution system includes a key management server for managing secret keys and public keys corresponding to given attribute values. Application, pp. 14, ll. 14-19, Fig. 1, item 10. A user terminal accesses the key management server to obtain attribute secret keys generated based on the secret keys. Application, pp. 14, ll. 20-24, Fig. 1, item 30. Furthermore, the attribute secret keys correspond to attributes identifying the user terminal. Application, pp. 12, ll. 13-18.

Claim 2 is dependent on claim 1 and recites that the provider terminal distributes the encrypted content without specifying an address of the user terminal that is to receive the encrypted content. Application, pp. 23, ll. 19-26.

Independent claim 4 recites a server that includes a key storage for storing secret keys and public keys corresponding to predetermined attribute values. Application, pp. 12, ll. 13-18 and Fig. 2, item 12. The server also includes an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret keys corresponding to the set of attribute values based on secret keys corresponding to the attribute values among the secret keys stored in the key storage. Application, pp. 12, ll. 9-18 and Fig. 2, item 11. A sending/receiving unit receives the set of attribute values from a given user terminal and sends the attribute secret

keys generated by the attribute secret key generator to the user terminal. Application, pp. 7, ll. 8-11. Furthermore, the attribute values identify the user terminal. Application, pp. 10, ll. 30 - pp. 11, ll. 2.

Independent claim 6 recites an information processing apparatus that includes a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes identifying a recipient to which a content is to be sent and using the public keys to generate criteria keys that can be decrypted by secret keys corresponding to the public keys. Application, pp. 12, ll. 12-20, pp. 18, ll. 9-14 and Fig. 2, item 22. The apparatus also includes an encrypted content generator for encrypting the content based on the criteria keys. Application, pp. 13, ll. 3-11 and Fig. 2, item 21. Furthermore, a sending unit is used to send the encrypted content without specifying any recipient of the content via a network. Application, pp.7, ll. 18-20.

Independent claim 9 recites an information processing apparatus receiving a content distributed over a network. Application, Fig. 1. The apparatus includes a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying the information processing apparatus. Application, pp. 7, ll. 26 - pp.8, ll. 2. The attribute secret keys are generated based on the secret keys. Application, pp.8, ll. 1-2. A decryptor is used to obtain an encrypted content and decrypt the content based on the attribute secret keys.

Application, pp.8, ll. 2-3, pp. 13, ll. 18-24 and Fig. 2, item 32.

Independent claim 20 recites an information distribution system including a service provider managing secret keys and public keys for given attribute values. Application, pp. 8, ll. 18-20, Fig. 8, item 800. The system also includes a plurality of user terminals for accessing the service provider to obtain attribute secret keys corresponding to attributes identifying the user terminals. Application, pp. 8, ll. 20-23, pp.14, ll. 20-24, Fig. 1, item 30. The attribute secret keys are generated based on the secret keys. Application, pp.8, ll. 1-2. Furthermore, a given one of the user terminals generates an encrypted content and sends the encrypted content to one or more of the other user terminals. Application, pp. 9, ll. 6-12, Fig. 8, item 810. The encrypted content is decryptable by the other user terminals having the attribute secret keys corresponding to given attributes by means of the public keys. Application, pp. 9, ll. 12-16.

Independent claim 21 recites an information distribution system including a key management server for managing secret keys and public keys for given attribute values. Application, pp. 14, ll. 14-19, Fig. 1, item 10. The system also includes a plurality of user terminals for accessing the key management to obtain attribute secret keys corresponding to attributes identifying the user terminals. Application, pp. 8, ll. 20-23, pp.14, ll. 20-24, Fig. 1, item 30. The attribute secret keys are generated based on the secret keys. Application, pp.8, ll. 1-2. Furthermore, a given one of the user terminals generates a group key and

sends the group key to one or more of the other user terminals and provides a content. Application, pp. 9, ll. 6-12, Fig. 10, item 1010. The encrypted group key is decryptable by the other user terminals having the attribute secret keys corresponding to given attributes by means of the public keys. Application, pp. 9, ll. 12-16.